WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Comprehensive Analysis of Image Encryption and Decryption Using J Component Methodology

[1] Meet Raval, [2] Yogesh Pargai, [3]Suraj Tiwari

[1]MC2223091, [2]MC2223079, [3]MC2223121
ASM IMCOST

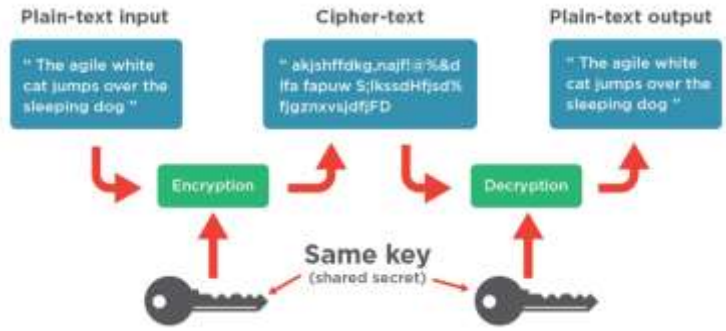
ABSTRACT:

Image encryption is an important aspect of protecting digital images from unauthorized access and ensuring confidentiality. A popular image encryption technique is the Arnold cat mapping technique, a chaos map-based approach that offers robust cryptographic properties. Arnold Cat's mapping technique is based on the concept of chaos theory and uses chaos maps to generate pseudorandom sequences that are highly sensitive to initial conditions. Arnold Cat maps are two-dimensional chaotic maps that manipulate images by rearranging pixels in a non-linear and deterministic way. The algorithm uses a permutation operation to periodically and repeatedly swap pixel positions, creating a chaotic pattern that spreads image pixels across the image. Arnold's cat mapping method offers several desirable properties for image encoding. First, because the encryption process is based on the chaotic behavior of the Arnold Cat card, it offers a high level of security as the encrypted image is resistant to attacks such as brute force and statistical analysis. will be Second, this technique offers excellent key confidentiality. A slight change in the encryption key produces a completely different encrypted image, ensuring confidentiality of the image data. Third, the technique has high cryptographic speed because permutation operations can be efficiently implemented using simple arithmetic operations.

Keywords: Arnold Cat Mapping, Chaotic Techniques, Cryptography , Encryption , Decryption.

INTRODUCTION:

Encryption is the process of transforming the original data, which is called plaintext, into encrypted data called ciphertext [1]. Different techniques are used to fulfill the data's own features of each data type. Many encryption algorithms are used to protect and encipher text data, such as the classical cipher system. Digital images are used in many communication applications, therefore the protection of the content of these images become very important. Image encryption is a technique which involves coding the original image (plain image) to another un-understanding image (cipher image). This technique must be provided by decoding the cipher image to plain image without losing data or image properties [3]. A diverse set of applications rely on digital image encryption and use various algorithms to protect the content and information of original images from unauthorized users. There are different types of encryption algorithms according to plaintext messages; some used for text data and not suitable for other multimedia data such as digital image. Other types used for images and not suitable for text data. Due to the powerful attributes of images, such as vast data capacity, great redundancy, and high correlation among pixels, encryption algorithms cannot be directly applied to images because of their large size. These algorithms require a significant amount of time when used with images. Another problem is that the decrypted text must be identical to the original text. However, this requirement is not necessary for image data. Due to the characteristic of human perception, a decrypted image containing small distortion is usually acceptable [4]. This paper presents textual encryption algorithms, such as the Vigenère and Hill cipher systems, which have been adapted and enhanced to encrypt and decrypt color digital images.The proposed system provides security to ensure that the original image can only be viewed or obtained by authorized individuals, integrity to guarantee that the image has not been altered, and confidentiality to ensure that the image remains secure during transmission.. In this research, we use an algorithm which is used with raw data, and used in digital image Encryption and Decryption with some advances that are suitable with digital images. In this paper we try to overcome the limitations of AES and RSA in the encryption and decryption of digital images.



LITERATURE SURVEY:

Sr.no	Title & author name	Methodology	Applications	Pros,Cons,Challenges
1.	Guo, Jiun-In. "A new chaotic key-based design for image encryption and decryption." *2000 IEEE international symposium on circuits and systems (ISCAS)*. Vol. 4. IEEE, 2000.	Chaotic Key-Based Design for Image Encryption and Decryption.	encryption and decryption process simulation	• It is possible to look at the simulation of encryption and decryption process happening at the backend. • Complex system structure
2.	M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki , "A Modified AES Based Algorithm for Image Encryption	Modified AES Based Algorithm	Can be realizes both on hardware and software without any difficulties.	• W7 gives better encryption results in terms of security against statistical analysis attacks. • The key stream generator has an important influence on the encryption performance • overcome the problem of textured zones
3.	Radhadevi, P., and P. Kalpana. "Secure image encryption using AES." *International Journal of Research in Engineering and Technology* 1.2 (2012): 115-117.	AES algorithm	Aes operations in image encryption and decryption	• Offers enhanced security • Offers flexibility allowing different key sizes
4.	Amador, Jose J., and Robert W. Green. "Symmetric-key block cipher for image and text cryptography." *International Journal of Imaging Systems and Technology* 15.3 (2005): 178-188.	NASA/Kennedy Cipher (N/KC)	As it is a new cipher method its applications are yet to be defined.	• Empirical results are presented on N/KC's ability of encrypting and decrypting text data in the form of vectors and documents. • management of the public-key and its storage is an on-going issue
5.	Padate, Roshni, and Aamna Patel. "Image encryption and decryption using AES algorithm." *International Journal of Electronics and*	AES and DES ,Block ciphers	Less time required for computation and a little stable method.	AES-128 offers many sufficiently enough number of keys for exhaustive search impractical for many decades

	Communication Engineering & Technology (2015): 23-29.			
6.	Sankhe, Pranjali, et al. "An image cryptography using henon map and arnold cat map." *Int. Res. J. Eng. Technol* 5.4 (2018).	Henon map Arnold cat map	Real time secure transmission system	● Highly sensitive to initial values and parameters ● Complex system since key value is generated using henon map and pixel shuffling is done using Arnold cat map.
7.	Hariyanto, Eko, and Robbi Rahim. "Arnold's cat map algorithm in digital image encryption." *International Journal of Science and Research (IJSR)* 5.10 (2016): 1363-1365.	Chaos based encryption - Arnold's Cat Map	A little more security to the aes encrypted images.	● This method can safeguard the image without reducing the value or information of a digital image that is secured
8.	Arab, Alireza, Mohammad Javad Rostami, and Behnam Ghavami. "An image encryption method based on chaos system and AES algorithm." The Journal of Supercomputing 75 (2019): 6663-6682.	Arnold Chaos sequence for key generation Encryption using AES algorithm	A little more security to the aes encrypted images as aes sometimes fail to do alone the task of encryption as of digitally.	● Resists Brute force attacks ● Small changes in original image and key leads to changes in the encrypted image and original cannot be accessed
9.	"A REVIEW ON IMAGE ENCRYPTION AND DECRYPTION"SaimaRafat Bhandari, ZarinaBegam K Mundargi	AES algorithm	Keystream cipher	Increase the performance Of the encryption technique.
10.	Davis, R. "The data encryption standard in perspective." *IEEE Communications Society Magazine* 16.6 (1978): 5-9.	DES	How the environment around des works and its various applications	objectives of additional standards to be developed within the computer security program
11.	Hurley, Neil, Zunping Cheng, and Mi Zhang. "Statistical attack detection." *Proceedings of the third ACM conference on Recommender systems*. 2009.	Statistical detection techniques	Detection of profile injection attacks	● Exploit explicit vulnerabilities ● attack and detection can result in an arms race scenario between the system manager and attacker.
12.	Shah, Tariq, and Sajjad Shaukat Jamal. "An improved chaotic cryptosystem for image encryption and digital watermarking." *Wireless personal communications*.	Enhanced chaos range map-Chaotic ILS encryption	Prevention against signal processing attacks and operations	● resist against the differential attacks and robustness against different signal processing attacks and operations ● Vulnerability to brute force attacks

13.	Morkel, Tayana, Jan HP Eloff, and Martin S. Olivier. "An overview of image steganography." *ISSA*. Vol. 1. No. 2. 2005.	Stenographic techniques	Image,data,text,audio ,video hiding to secure its data.	• Independent of file format • Robustness against image manipulation • Robustness against statistical attacks
14.	Bhowmik, Sandeep, and Sriyankar Acharyya. "Image encryption approach using an improved chaotic system incorporated with differential evolution and genetic algorithm." *Journal of Information Security and Applications* 72 (2023): 103391.	Meta-heuristic techniques	the chaotic performance of the key-strings used in confusion and diffusion operations.	• hereby stands against all kinds of statistical and differential attacks including brute force. • Limited to black and white images • Time complexities need to be reduced
15.	Zhu, Zhi-liang, et al. "A chaos-based symmetric image encryption scheme using a bit-level permutation." *Information Sciences* 181.6 (2011): 1171-1186.	Bit-level permutation	Applied for encryption to vulnerability of permutation-only ciphers to known/chosen plaintext attacks	• superior security and computational efficiency. • permutations and diffusions are performed several times in alternation to achieve a satisfactory security level.
16.	Khade, Pawan N., and Manish Narnaware. "3D chaotic functions for image encryption." *International Journal of Computer Science Issues (IJCSI)* 9.3 (2012): 323.	3D chaotic algorithms and use of Chebyshev map to generate keys	Better security of the image as the use of 3D Logistics map provides the higher key sensitivity .	• Provides higher key sensitivity • The system is more complex as it uses 3 additional keys • 3D Arnold's Cat map is used for additional scrambling and substitution
17.	Kankonkar, Jyoti TG, and Nitesh Naik. "Image security using image encryption and image stitching." *2017 International Conference on Computing Methodologies and Communication (ICCMC)*. IEEE, 2017.	Image stitching	double layered protection to the images that are being transferred	• Difficult for the attackers to steal the information conveyed through the user to the receiver
18.	Anak Agung Putri Ratna, Anak, et al. "Chaos-based image encryption using Arnold's cat map confusion and Henon map diffusion." *Advances in Science, Technology and Engineering Systems* 6.1 (2021): 316-326	Arnold's cat map Henon map	Keep medical records confidential	• Less complexity for confusion and diffusion • Confusion method is not secure enough

19.	Munir, Rinaldi. "A secure fragile video watermarking algorithm for content authentication based on Arnold Cat Map." *2019 4th International Conference on Information Technology (InCIT)*. IEEE, 2019.	XOR function Chaos map	encrypted watermark is embedded by modifying pixel values of video frames. Detection of tampering on the watermarked video.	• Useful to detect the tampered region • watermark need to be replicated by duplicating it a number of times in order to produce a new watermark identical to original
20.	Elshamy, Elsayed M., et al. "Secure VoIP System Based on Biometric Voice Authentication and Nested Digital Cryptosystem using Chaotic Baker's map and Arnold's Cat Map Encryption." *2017 International Conference on Computer and Applications (ICCA)*. IEEE, 2017.	Baker's map.	VoIP security in two levels	• passing the encrypted file through OFDM framework with variant SNR that the performance evaluation elements are similar in the sender and receiver, and this means the efficiency of encryption and decryption process.

EXISTING METHODS:

There are several existing methods for image encryption, some of which are:

1. ***Substitution-permutation network (SPN) encryption:*** This method involves using a combination of substitution and permutation operations to encrypt an image.
2. ***Feistel network-based encryption:*** This method is based on the use of Feistel networks, which involve splitting an image into two halves, and then encrypting each half using a key-dependent function.
3. ***Chaos-based encryption:*** This method involves using chaotic systems to generate the encryption key, which is then used to scramble the image.
4. ***Public key-based encryption:*** This method involves using a public key to encrypt an image, which can then only be decrypted using the corresponding private key.
5. ***DNA-based encryption:*** This method involves encoding an image using DNA sequences, which can then be decoded using DNA sequencing technology.
6. ***Steganography-based encryption:*** This method involves hiding an image within another image, so that it is not visible to the naked eye, and can only be accessed using a secret key.
7. ***Quantum-based encryption:*** This method involves using quantum cryptography principles to encrypt an image, which ensures high levels of security.

PROPOSED WORK:

For encryption**:**

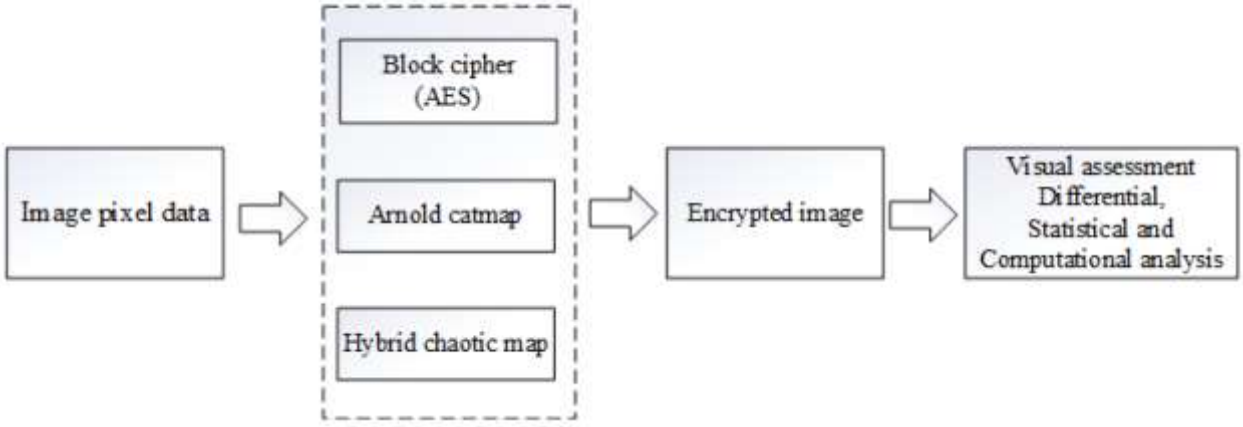
1. Input the original image to be encrypted.
2. Define the encryption parameters, such as the number of iterations and the encryption key.Apply the Arnold Cat mapping algorithm to permute the pixels of the original image. The algorithm typically involves the following steps:
3. Calculate the new position of each pixel using the following formulas:

New_X = (a * X + b * Y) mod Image_Width

New_Y = (c * X + d * Y) mod Image_Height

where X and Y represent the original coordinates of the pixel, and a, b, c, d are the parameters of the Arnold Cat map obtained from the encryption key. Update the pixel values in the new positions to obtain the encrypted image.

4. Repeat the permutation process for the desired number of iterations.
5. Output the encrypted image.



For decryption:

1. Input the encrypted image to be decrypted.
2. Define the decryption parameters, such as the number of iterations and the decryption key (which should match the encryption key).Apply the inverse Arnold Cat mapping algorithm to reverse the permutation of the encrypted image. The algorithm typically involves the following steps:

   a. Calculate the original position of each pixel using the following formulas:

   Old_X = (d * X - b * Y) mod Image_Width

   Old_Y = (-c * X + a * Y) mod Image_Height

   where X and Y represent the encrypted coordinates of the pixel, and a, b, c, d are the parameters of the Arnold Cat map obtained from the decryption key. Update the pixel values in the original positions to obtain the decrypted image.

3. Repeat the inverse permutation process for the desired number of iterations.
4. Output the decrypted image.

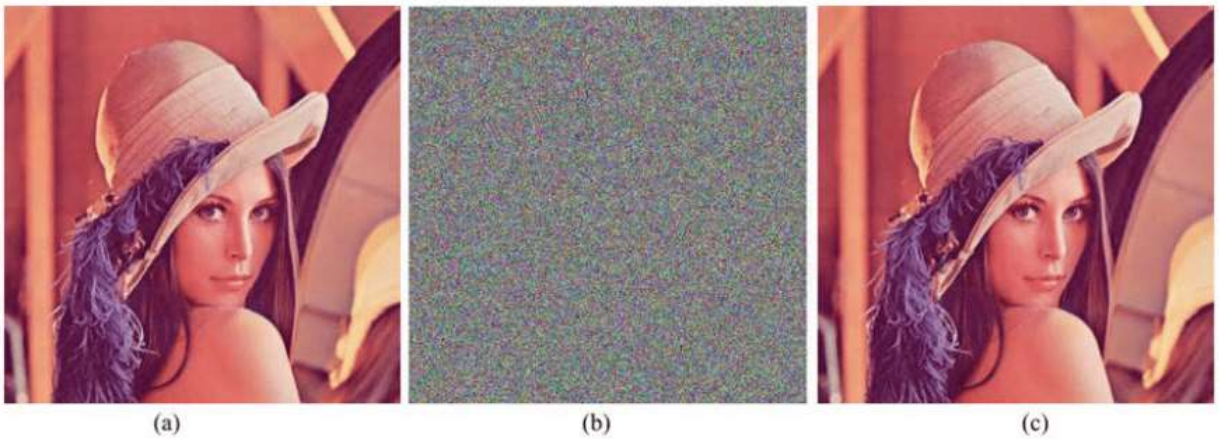


Fig 2a: original image Fig 2b: encrypted image of the original image Fig 2c: decrypted image of the encrypted image produced

REFERENCES:

[1] Guo, Jiun-In. "A new chaotic key-based design for image encryption and decryption." *2000 IEEE international symposium on circuits and systems (ISCAS)*. Vol. 4. IEEE, 2000.

[2] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki , "A Modified AES Based Algorithm for Image Encryption",2007 .
[3] Radhadevi, P., and P. Kalpana. "Secure image encryption using AES." *International Journal of Research in Engineering and Technology* 1.2 (2012): 115-117.

[4]Padate, Roshni, and Aamna Patel. "Image encryption and decryption using AES algorithm." *International Journal of Electronics and Communication Engineering & Technology* (2015): 23-29.

[5] Amador, Jose J., and Robert W. Green. "Symmetric-key block cipher for image and text cryptography." *International Journal of Imaging Systems and Technology* 15.3 (2005): 178-188.

[6] Sankhe, P., Pimple, S., Singh, S., & Lahane, A. (2018). An image cryptography using henon map and arnold cat map. Int. Res. J. Eng. Technol, 5(4).

[7] Hariyanto, Eko, and Robbi Rahim. "Arnold's cat map algorithm in digital image encryption." International Journal of Science and Research (IJSR) 5.10 (2016): 1363-1365.

[8]"A REVIEW ON IMAGE ENCRYPTION AND DECRYPTION"SaimaRafat Bhandari, ZarinaBegam K Mundargi

[9]Arab, Alireza, Mohammad Javad Rostami, and Behnam Ghavami. "An image encryption method based on chaos system and AES algorithm." The Journal of Supercomputing 75 (2019): 6663-6682.

[10]Davis,R.,"TheDataEncryptionStandardinPerspective,"Proceedings of Communication Society magazine,IEEE

[11]Hurley, Neil, Zunping Cheng, and Mi Zhang. "Statistical attack detection." *Proceedings of the third ACM conference on Recommender systems*. 2009.

[12]Shah, Tariq, and Sajjad Shaukat Jamal. "An improved chaotic cryptosystem for image encryption and digital watermarking." *Wireless personal communications*.

[13]Morkel, Tayana, Jan HP Eloff, and Martin S. Olivier. "An overview of image steganography." *ISSA*. Vol. 1. No. 2. 2005.

[14]Bhowmik, Sandeep, and Sriyankar Acharyya. "Image encryption approach using improved chaotic system incorporated with differential evolution and genetic algorithm." *Journal of Information Security and Applications* 72 (2023): 103391.

[15]Zhu, Zhi-liang, et al. "A chaos-based symmetric image encryption scheme using a bit-level permutation." *Information Sciences* 181.6 (2011): 1171-1186.

[16]Khade, Pawan N., and Manish Narnaware. "3D chaotic functions for image encryption." *International Journal of Computer Science Issues (IJCSI)* 9.3 (2012): 323.

[17]Kankonkar, Jyoti TG, and Nitesh Naik. "Image security using image encryption and image stitching." *2017 International Conference on Computing Methodologies and Communication (ICCMC)*. IEEE, 2017.

[18]Anak Agung Putri Ratna, Anak, et al. "Chaos-based image encryption using Arnold's cat map confusion and Henon map diffusion." *Advances in Science, Technology and Engineering Systems* 6.1 (2021): 316-326

[19]Munir, Rinaldi. "A secure fragile video watermarking algorithm for content authentication based on Arnold Cat Map." *2019 4th International Conference on Information Technology (InCIT)*. IEEE, 2019

[20]Elshamy, Elsayed M., et al. "Secure VoIP System Based on Biometric Voice Authentication and Nested Digital Cryptosystem using Chaotic Baker's map and Arnold's Cat Map Encryption." *2017 International Conference on Computer and Applications.*